Capitolo 7

Metodi generali di risoluzione: Lagrange e Vandermonde

7.1 Lagrange e la risoluzione algebrica delle equazioni

Lagrange dedicò diverse memorie alle equazioni algebriche ed i suoi contributi principali riguardano: 1) l'aver messo in luce i tratti comuni a tutti i metodi di soluzione algebrica delle equazioni fino allora escogitati riuscendo a mostrare l'importanza delle permutazioni effettuate sulle radici di un'equazione come linea guida per decidere della risolubilità di un'equazione e come base di un metodo unificante di risoluzione; 2) lo studio di metodi per la risoluzione *numerica* delle equazioni algebriche. Il lavoro fondamentale di Lagrange per il primo aspetto è la corposa memoria *Réflexions sur la Résolution Algébrique des équations* [1] pubblicata in due parti tra il 1770 ed il 1771 mentre per la risoluzione numerica, il testo più importante è il *Traité de la Résolution numerique des equations* [2] in cui Lagrange amplia il contenuto di memorie apparse sull'argomento a partire dal 1769 e che pure dedica una Nota (la XIII) all'esposizione dei risultati più originali delle *Réflexions*. L'importanza del lavoro di Lagrange nel proporre un punto di vista nuovo ed unificante da cui saprà trarre profitto Galois è stata sottolineata in diversi lavori storici come [3], dedicato ad un'ampia panoramica dei contributi di Lagrange, [4] che esamina, tra le altre cose, l'influenza dell'opera di Lagrange nello sviluppo della teoria di Galois e [5] dove si evidenziò il contributo pionieristico di Lagrange alla teoria delle permutazioni. Ci soffermeremo alquanto in questo capitolo sul contenuto delle *Réflexions* che in effetti ha esercitato un influsso notevole sui matematici delle generazioni successive ed è stato fonte di ispirazione per molti.

Le *Réflexions* si articolano in quattro grandi sezioni: la prima e la seconda

trattano i metodi noti per la risoluzione di equazioni di terzo e quarto grado esaminati alla luce di un nuovo principio guida: il comportamento delle radici di un'equazione ausiliaria sotto l'azione di permutazioni tra le radici dell'equazione proposta. La terza sezione esamina il comportamento dei metodi più generali per la risoluzione di equazioni algebriche—metodi di Tschirnhaus, Eulero e Bezout—di fronte alla risoluzione delle equazioni di quinto grado cercando di comprendere i motivi dei loro fallimenti. Infine la quarta sezione, la più innovativa, considera il problema generale delle trasformazioni di equazioni di grado qualunque che portano ad abbassarne il grado e quindi a permetterne la risolubilità algebrica.

Lagrange dichiara sin dall'introduzione delle *Réflexions* l'obiettivo che il suo lavoro si prefigge: *In questa Memoria mi propongo di esaminare i metodi differenti trovati sino al momento presente per la risoluzione algebrica delle equazioni, di ridurli a principî generali e di far vedere a priori perché questi metodi hanno successo per il terzo ed il quarto grado e sono in difetto per i gradi maggiori.*

Questo esame presenta un doppio vantaggio: da un lato servirà a gettare più luce possibile sulle soluzioni note di terzo e quarto grado; d'altra parte esso sarà di aiuto a quanti vorranno occuparsi della soluzione dei gradi più alti, fornendo loro diversi punti di vista sull'argomento e soprattutto risparmiando loro un gran numero di passi falsi e tentativi inutili.[1] ([1], pp. 206-207)

In questo passo si trova la parola chiave per comprendere l'approccio di Lagrange al problema della risoluzione algebrica delle equazioni: *a priori*. Occorre comprendere *a priori* perché i metodi proposti funzionano e non limitarsi, come si era sempre fatto sino a quel momento, ad un'analisi *a posteriori*, cioè a risultato ottenuto, della validità del metodo proposto. Solo ponendosi seriamente la domanda del *perché* un certo metodo funzioni è possibile guidare i passi successivi della ricerca, volti alla risoluzione di equazioni di grado maggiore.

Vediamo l'esame che Lagrange opera di due metodi di soluzione per equazioni di terzo grado: il metodo di Viète e quello di Tschirnhaus. Mentre il primo è per sua natura limitato alla soluzione di equazioni di grado $n = 3$, il secondo ricorre invece ad una trasformazione generalizzabile a valori più grandi di n e dunque promettente per ottenere una soluzione algebrica in generale. Se torniamo ai metodi esposti nel Capitolo 4 di queste dispense abbiamo visto come le radici dell'equazione da risolvere vengano espresse in termini delle radici di un'equazione ausiliaria (che Lagrange chiama *ridotta*, *réduit*, *perché è l'equazione alla cui soluzione si riduce quella dell'equazione di partenza.*[2] ([1], p. 213), la cui soluzione è nota. Lagrange ha l'idea vincente di affrontare la strada in senso inverso, esprimendo le radici della ridotta in termini di quelle dell'equazio-

[1] Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux, et de faire voir à priori pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défeaut pour les dégres ultérieurs Cet examen aura un double avantage: d'un côté il servira à répandre une plus grande lumière sur les résolutions connues du troisième et du quatrième degré; de l'autre il sera utile à ceux qui voudront s'occuper de la résolution des dégres supérieurs, on leur furnissant différentes vues pour cet objet et en leur épargnant surtout un grand nombre de pas et de tentatives inutiles.

[2] s'appelle la réduite (...) parce que c'est à sa résolution que se réduit celle de la proposée.

ne proposta per ricavare le proprietà della ridotta che permettono la soluzione dell'equazione proposta.

Per le equazioni di terzo grado Lagrange considera la forma completa

$$x^3 + mx^2 + nx + p = 0 \tag{7.1}$$

e chiama x_1, x_2 ed x_3 le sue radici[3]. Effettuata la trasformazione $x = x' - \frac{m}{3}$, (7.1) si trasforma, come è noto, in

$$x'^3 + n'x' + p' = 0$$

dove i coefficienti n' e p' si esprimono in funzione di quelli dati attraverso le relazioni

$$n' = n - \frac{m^2}{3} \qquad p' = p - \frac{mn}{3} + \frac{2m^3}{27}.$$

A questo punto si effettua la trasformazione di Viète $x' = y - \frac{n'}{3y}$ e si ottiene la ridotta

$$y^6 + p'y^3 - \frac{n'^3}{27} = 0 \tag{7.2}$$

che, detta

$$r := \sqrt[3]{-\frac{p'}{2} + \sqrt{\frac{p'^2}{4} + \frac{n'^3}{27}}}, \tag{7.3}$$

è risolta da

$$y_1 = r \qquad y_2 = \alpha r \qquad y_3 = \alpha^2 r = \beta r \tag{7.4}$$

dove α e $\beta = \alpha^2$ sono le radici cubiche *complesse* dell'unità, distinte da 1. Grazie a (7.4) ed effettuando a ritroso le trasformazioni che hanno condotto alle y_i, Lagrange è in grado di ricavare

$$\begin{cases} x_1 = -\frac{m}{3} + r - s \\ x_2 = -\frac{m}{3} + \alpha r - \frac{s}{\alpha} \\ x_3 = -\frac{m}{3} + \beta r - \frac{s}{\beta} \end{cases} \tag{7.5}$$

dove si è posto $s := \frac{n'}{3r}$. Lagrange mette in atto la sua idea di esprimere r come funzione delle x_i e per questo inizia ad osservare che, da (7.5), si ha

$$\begin{aligned} x_1 - x_2 &= (1-\alpha)\left(r + \tfrac{s}{\alpha}\right) \\ x_1 - x_3 &= (1-\beta)\left(r + \tfrac{s}{\beta}\right) \end{aligned}$$

da cui si ottiene dapprima

$$\alpha r + s = \frac{\alpha(x_1 - x_2)}{1-\alpha} \qquad \text{e} \qquad \beta r + s = \frac{\beta(x_1 - x_3)}{1-\beta}$$

[3]Nell'originale Lagrange indica le radici di (7.1) con a, b, c. Ho proferito adottare una notazione più vicina a quella attuale ed anche a quella impiegata da Lagrange nella Nota XIII del *Traité*.

e poi, sottraendo tra loro queste equazioni con alcuni passaggi diretti

$$r = \frac{x_1}{(1-\alpha)(1-\beta)} + \frac{\alpha x_2}{(\alpha-1)(\alpha-\beta)} + \frac{\beta x_3}{(\beta-\alpha)(\beta-1)}.$$

Per semplificare ulteriormente quest'equazione Lagrange osserva che, dal momento che 1, α e β sono radici di $x^3 - 1 = 0$ si può scrivere

$$x^3 - 1 = (x-1)(x-\alpha)(x-\beta)$$

che, dopo una derivazione, fornisce

$$3x^2 = (x-\alpha)(x-\beta) + (x-1)(x-\beta) + (x-1)(x-\alpha) :$$

calcolando questa derivata in $x = 1$, $x = \alpha$ ed $x = \beta$ si ottengono le relazioni

$$3 = (1-\alpha)(1-\beta) \quad 3\alpha^2 = (\alpha-1)(\alpha-\beta) \quad 3\beta^2 = (\beta-1)(\beta-\alpha)$$

da cui è possibile infine ottenere

$$r = \frac{x_1 + \alpha x_3 + \beta x_2}{3} =: y_1, \tag{7.6}$$

che rappresenta la relazione tra la radice y della ridotta e le radici dell'equazione di partenza. Lagrange è ora in grado di rispondere alla domanda che serve a svelare la *ratio* nascosta dietro questo metodo di soluzione delle equazioni di terzo grado. Perché, in primo luogo, la ridotta è un'equazione di sesto grado? È in questo momento che entrano in scena le permutazioni

Si vede allora da questa espressione perché la ridotta è necessariamente di sesto grado; infatti, siccome tale ridotta non dipende immediatamente dalle radici x_1, x_2, x_3 dell'equazione proposta ma solo dai coefficienti m, n e p nei quali le tre radici entrano in modo equivalente, è chiaro che nell'espressione di y deve essere possibile scambiare tra loro a piacere le quantità x_1, x_2, x_3; di conseguenza la quantità y dovrà avere tanti valori distinti quanti se ne possono formare con tutte le permutazioni possibili tra le tre radici x_1, x_2 e x_3; è noto dalla teoria delle combinazioni che il numero di permutazioni, cioè degli arrangiamenti differenti di tre cose è $3 \cdot 2 \cdot 1$; dunque anche la ridotta in y deve essere di grado $3 \cdot 2 \cdot 1$, cioè del sesto[4] ([1], pp. 215-216). Dunuqe, permutando tra loro x_1, x_2 ed x_3 in (7.6), sono ugualmente radici della ridotta

$$y_2 = \frac{x_1+\alpha x_3+\beta x_2}{3}, \quad y_3 = \frac{x_2+\alpha x_1+\beta x_3}{3} \quad y_4 = \frac{x_2+\alpha x_3+\beta x_1}{3}$$
$$y_5 = \frac{x_3+\alpha x_2+\beta x_1}{3}, \quad y_6 = \frac{x_3+\alpha x_1+\beta x_2}{3}$$

[4]On voit d'abord par cette expression de y pourquoi la réduite est nécessairement du sixième degré; car comme cette réduite ne dépend pas immédiatement des racines x_1, x_2, x_3, mais seulement des coefficients m, n, p, où les trois rscines entrent également, il est clair que dans l'expression de y on doit pouvoir échanger à volonté les quantités x_1, x_2, x_3 entre elles; par conséquent la quantité y devra avoir autant de valeurs différentes que l'on pourra former par toutes les permutations possibles dont les trois racines x_1, x_2, x_3 sont susceptibles; or on sait par la théorie des combinaisons que le nombre des permutations, c'est-à-dire des arrangements différents des trois choses, est $3 \cdot 2 \cdot 1$; donc la réduite doit étre aussi du degré , c'est-à-dire du sixième.

D'altra parte, che debba essere così è conseguenza della *arbitrarietà* con cui sono state associate le x_i alle radici della ridotta.

Chiarito dunque il motivo per cui la ridotta è di sesto grado, Lagrange risponde alla seconda domanda cruciale: perché la ridotta si può risolvere al modo di un'equazione di secondo grado o, meglio, perché si spezza nella soluzione di un'equazione di secondo grado ed in una di terzo pura? Per rispondere, Lagrange richiama alcune proprietà fondamentali delle radici dell'unità α e β. Si ha infatti $\alpha = \beta^2$ e, dal momento che $\alpha^3 = \beta^3 = 1$, si hanno sia $\alpha\beta = 1$ che $\alpha^2 = \beta$. Grazie a queste relazioni si verifica che, moltiplicando y_1 per α prima e poi per β si ottengono y_6 ed y_4 mentre la stessa operazione eseguita a partire da y_2 porta ad y_3 ed y_5 per cui

$$y_6 = \alpha y_2 \quad y_4 = \beta y_2 \qquad y_3 = \alpha y_1 \quad y_5 = \beta y_1$$

che dimostra come, note *due* radici della ridotta, tutte le altre siano ottenibili moltiplicando queste per α e β. Lagrange può ora proporre un metodo generale di risoluzione per le equazioni di terzo grado che *non* dipende dalla particolare trasformazione adoperata. Partendo da (7.1) si *suppone* di poter esprimere le radici della ridotta come funzioni lineari delle radici di (7.1),

$$r_1 := Ax_1 + Bx_2 + Cx_3$$

dove le quantità A, B, C sono al momento incognite ma *indipendenti* dalle x_i. Eseguendo tutte le permutazioni possibili sulle $\{x_i\}$ si ottengono gli altri cinque valori

$$r_2 = Ax_1 + Bx_3 + Cx_2 \quad r_3 = Ax_2 + Bx_1 + Cx_3 \quad r_4 = Ax_2 + Bx_3 + Cx_1$$

ed

$$r_5 = Ax_3 + Bx_2 + Cx_1 \quad r_6 = Ax_3 + Bx_1 + Cx_2.$$

Si impone che la ridotta contenga solo potenze multiple di 3 dell'incognita per cui, se r risolve la ridotta, anche αr e βr la risolvono. Ora, chiedendo che $r_2 = \alpha r_1$ sia vera per *tutti* i possibili valori di $\{x_i\}$ equivale a chiedere $\alpha A = A$ e dunque $\alpha = 1$, mentre sappiamo che $\alpha \neq 1$. Similmente, la richiesta $\alpha r_1 = r_3$ fornisce $\alpha C = C$ che ancora imporrebbe $\alpha = 1$. Al contrario, se si impone $\alpha r_1 = r_4$ si ottiene $\alpha A = C$, $\alpha B = A$ ed $\alpha C = B$ per cui

$$C = \alpha A = \alpha^2 B = \alpha^3 C,$$

consistente con $\alpha^3 = 1$. Per semplicità è sempre possibile porre $A = 1$ e ricavare le due radici fondamentali della ridotta nella forma

$$r =: r_1 = x_1 + \alpha x_2 + \beta x_3 \qquad s := r_2 = x_1 + \alpha x_3 + \beta x_2. \tag{7.7}$$

La ridotta, dovendo avere r, αr, $\beta r = \alpha^2 r$, s, αs e $\beta s = \alpha^2 r$ come radici si fattorizza come

$$(y - r)(y - \alpha r)(y - \alpha^2 r)(y - s)(y - \alpha s)(y - \alpha^2 s) = (y^3 - r^3)(y^3 - s^3) = 0$$

che si riscrive come

$$y^6 - (r^3 + s^3)y^3 + r^3 s^3 = 0. \tag{7.8}$$

Tutto questo non sarebbe molto utile se non fosse possibile trovare espressioni di r^3 ed s^3 in funzione dei coefficienti di (7.1) e per questo entrano in gioco le formule di Viète-Girard ed i teoremi newtoniani (per una dimostrazione di questi teoremi, si veda la sezione 7.5). Da (7.7) Lagrange ottiene

$$r^3 = x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3\alpha(x_2x_1^2 + x_3x_2^2 + x_1x_3^2) + 3\beta(x_1x_2^2 + x_2x_3^2 + x_3x_1^2)$$

e, scambiando tra loro α e β,

$$s^3 = x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3\alpha(x_3x_1^2 + x_2x_3^2 + x_1x_2^2) + 3\beta(x_1x_3^2 + x_3x_2^2 + x_2x_1^2).$$

Seguendo alla lettera Lagrange, poniamo

$$L := x_1^3+x_2^3+x_3^3+6x_1x_2x_3 \qquad M := (x_2x_1^2+x_3x_2^2+x_1x_3^2) \qquad N := x_1x_2^2+x_2x_3^2+x_3x_1^2$$

si ottiene

$$r^3 + s^3 = 2L + 3(\alpha + \beta)(M + N)$$

e siccome la somma delle tre radici di $x^3 - 1 = 0$ è nulla, deve essere

$$1 + \alpha + \beta = 1 + \alpha + \alpha^2 = 0 \tag{7.9}$$

sicché in definitiva

$$r^3 + s^3 = 2L - 3(M + N).$$

D'altro canto, sempre utilizzando (7.9), si verifica che

$$r^3 s^3 = L[L - 3(M + N)] + 9[(M + N)^2 - 3MN].$$

Ora, i coefficienti L, $M + N$ ed MN sono funzioni *simmetriche* delle radici di (7.1) e dunque sono esprimibili in funzione dei soli *coefficienti* dell'equazione (7.1) grazie al teorema fondamentale delle funzioni simmetriche (per una dimostrazione, si veda la sezione 7.6). Infatti, dalle formule di Viète-Girard sappiamo che

$$m = -(x_1 + x_2 + x_3) \quad n = x_1x_2 + x_1x_3 + x_2x_3 \qquad p = -x_1x_2x_3$$

da cui si deduce

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = m^2 - 2n$$

e

$$\begin{aligned} &x_1^3 + x_2^3 + x_3^3 = \\ &= (x_1 + x_2 + x_3)^3 - 3(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) - 3x_1x_2x_3 = -m^3 + 3mn - 3p \end{aligned}$$

da cui anche segue

$$x_1^3x_2^3 + x_1^3x_3^3 + x_2^3x_3^3 = n^3 - 3mnp + 3p^2$$

e quindi, in definitiva,

$$L = -m^3 + 3mn - 9p, \quad M + N = 3p - mn \quad MN = n^3 + p(m^2 - 6mn) + 9p^2$$

che permettono di dedurre le espressioni di $r^3 + s^3$ ed $r^3 s^3$ in funzione dei coefficienti della (7.1):

$$y^6 + (2m^3 - 9mn + 27p)y^3 + (m^2 - 3n)^3 = 0. \tag{7.10}$$

Dunque, ponendo $z := y^3$ occorre risolvere l'equazione di secondo grado

$$z^2 + (2m^3 - 9mn + 27p)z + (m^2 - 3n)^3 = 0 : \tag{7.11}$$

dette z_1 e z_2 le sue radici, poiché da (7.8) si ha che r ed s sono valori che risolvono l'equazione in y si potrà sempre scrivere

$$\begin{cases} r = x_1 + \alpha x_2 + \beta x_3 = \sqrt[3]{z_1} \\ s = x_1 + \alpha x_3 + \beta x_2 = \sqrt[3]{z_2} \\ \text{con} \\ -m = x_1 + x_2 + x_3 \end{cases} \tag{7.12}$$

che, sommate tra loro con il ricorso a (7.9), danno

$$x_1 = \frac{-m + \sqrt[3]{z_1} + \sqrt[3]{z_2}}{3};$$

similmente, se prima di sommare si moltiplica la prima delle (7.12) per β e la seconda per α o, viceversa, la prima per α e la seconda per β, si ottiene

$$x_2 = \frac{-m + \beta\sqrt[3]{z_1} + \alpha\sqrt[3]{z_2}}{3} \qquad x_3 = \frac{-m + \alpha\sqrt[3]{z_1} + \beta\sqrt[3]{z_2}}{3} :$$

siccome z_1 e z_2 sono funzioni dei coefficienti di (7.1), la risoluzione dell'equazione di terzo grado con il metodo di Lagrange è completata. Osserviamo che il metodo di Lagrange non ha come scopo principale quello di *semplificare* altri metodi quanto quello di trovare un principio comune a tutti i metodi escogitati per la soluzione algebrica delle equazioni di terzo grado.

7.2 Il metodo di Tschirnhaus

Dopo essersi occupato di un metodo di soluzione per equazioni di terzo grado modellato su di esse e dunque difficilmente esportabile ad equazioni di grado superiore, Lagrange dedica ampio spazio all'esposizione di altri metodi che, al contrario, sufficientemente generali da essere applicati anche alle equazioni di grado superiore. Nel dettaglio, Lagrange esamina i metodi di Tschirnhaus, di Eulero e di Bezout. Mi occuperò dell'esposizione del metodo di Tschirnhaus applicato alla soluzione delle equazioni di terzo grado che viene analizzato da Lagrange nei §§10-16 di [1]. Sugli *Acta Eruditorum* del 1683 era apparsa una

breve nota [7] dello scienziato tedesco Ehrenfried Walter von Tschirnhaus (1651-1708) che proponeva un metodo generale per la risoluzione di equazioni di grado qualunuqe. L'essenza del metodo è quella di generalizzare la trasformazione che permette di eliminare da un'equazione il termine che segue immediatamente quello di grado massimo. In questa trasformazione si effettuava un cambio di variabile $x \mapsto y = x + a$ in cui l'unico parametro libero presente a era determinato imponendo l'annullamento del termine di grado minore successivo a quello di grado massimo. Ora, Tschirnhaus ebbe l'idea di estendere la classe di trasformazioni in modo da poter eliminare quanti più termini possibili in un'equazione di grado n. In estrema sintesi, se con una trasformazione del tipo $x = y + a$ dipendente da *un* solo parametro libero a è possibile eliminare un termine da un'equazione grazie ad una scelta opportuna di a, trasformazioni del tipo

$$x^2 = bx + y + a \qquad x^3 = cx^2 + bx + y + a \qquad \text{ecc.}$$

possono essere impiegate per eliminare due, tre, ecc. termini da un'equazione e consentirne una semplificazione notevole. È chiaro che l'obiettivo del metodo è quello di trasformare un'equazione completa di grado n in un'equazione binomia del tipo $y^n = C$ le cui soluzioni, come dirà Lagrange, sono note immediatamente (*sur le champ*). Ora, questo metodo condurrà alla risoluzione di un sistema ausiliario di equazioni algebriche il cui grado, però, è destinato a salire oltre a quello dell'equazione proposta come notò per primo Leibniz, poco dopo la pubblicazione del lavoro di Tschirnhaus. Tuttavia, nel caso di equazioni di terzo grado la ridotta era di *secondo* grado e non di sesto grado e per Lagrange occorre considerare i motivi nascosti dietro questa riduzione per studiarne l'effettiva applicabilità ad equazioni di grado superiore al quarto. Lagrange espone dapprima il metodo seguendo le linee indicate sommariamente da Tschirnhaus per poi effettuarne l'analisi *a priori*. Si riparta dunque da (7.1) e si ponga

$$x^2 = bx + a + y \tag{7.13}$$

dove b ed a sono da determinare. Per questo, Lagrange moltiplica ambo i membri di (7.13) per x ottenendo

$$x^3 = bx^2 + ax + xy$$

e sostituisce il valore di x^2 dato da (7.13) ricavando infine

$$x^3 = (b^2 + a + y)x + b(a + y) : \tag{7.14}$$

sostituendo (7.13) e (7.14) in (7.1) si ottiene

$$(b^2 + mb + n + a + y)x + (b + m)(a + y) + p = 0$$

da cui si ricava x come funzione razionale di y, dei parametri della trasformazione e dei coefficienti dell'equazione proposta:

$$x = -\frac{(b + m)(a + y) + p}{b^2 + mb + n + a + y}.$$

Inserito in (7.1) questo valore di x si ottiene un'altra equazione di terzo grado in y

$$y^3 + Ay^2 + By + C = 0$$

in cui i coefficienti A, B e C sono legati ai parametri della trasformazione ed ai coefficienti dell'equazione proposta. In particolare,

$$A = 3a - mb - m^2 + 2n$$

e

$$B = 3a^2 - 2a(mb + m^2 - 2n) + nb^2 + (mn - 3p)b + n^2 - 2mp$$

sono i coefficienti da annullare in modo da ottenere un'equazione trasformata del tipo

$$y^3 + C = 0, \tag{7.15}$$

di soluzione immediata. Ora, da $A = 0$ si ottiene

$$a = \frac{mb + m^2 - 2n}{3}$$

che, sostituito in $B = 0$, fornisce l'equazione

$$(m^2 - 3n)b^2 + (2m^3 - 7mn + 9p)b + m^4 - 4m^2n + 6mp + n^2 = 0$$

per cui la determinazione dei parametri che individuano la trasformazione di Tschirnhaus è ricondotta alla soluzione di un sistema di secondo grado. Sin qui Lagrange non ha fatto altro che sviluppare, utilizzando il metodo di eliminazione, i calcoli necessari a portare a termine la trasformazione. Per quale motivo la ridotta è ora di secondo anziché di sesto grado? Lagrange affronta la questione a partire dal §15 di [1] ed osserva che (7.15) ha le soluzioni $-\sqrt[3]{C}$, $-\alpha\sqrt[3]{C}$ e $-\alpha^2\sqrt[3]{C}$ dove, al solito $\alpha \neq 1$ è una radice cubica dell'unità. Ora, queste radici debbono corrispondere alle radici x_1, x_2 ed x_3 di (7.1) ed il legame è proprio stabilito dalla trasformazione (7.13)

$$\begin{cases} x_1^2 = bx_1 + a - \sqrt[3]{C} \\ x_2^2 = bx_2 + a - \alpha\sqrt[3]{C} \\ x_3^2 = bx_3 + a - \alpha^2\sqrt[3]{C} \end{cases} \tag{7.16}$$

da cui si ricavano i valori di a e b, eliminando C. Moltiplicando la seconda delle equazioni (7.16) per α, la terza per α^2, sommando i risultati ed osservando che $\alpha^4 = \alpha$ e $\alpha^2 + \alpha + 1 = 0$ si otterrà

$$b = b_1 = \frac{x_1^2 + \alpha x_2^2 + \alpha^2 x_3^2}{x_1 + \alpha x_2 + \alpha^2 x_3}.$$

Ora, permutando tra loro le radici $\{x_i\}$, questa quantità assume i valori

$$b_2 = \frac{x_1^2 + \alpha x_3^2 + \alpha^2 x_2^2}{x_1 + \alpha x_3 + \alpha^2 x_2} \quad b_3 = \frac{x_2^2 + \alpha x_3^2 + \alpha^2 x_1^2}{x_2 + \alpha x_3 + \alpha^2 x_1} \quad b_4 = \frac{x_2^2 + \alpha x_1^2 + \alpha^2 x_3^2}{x_2 + \alpha x_1 + \alpha^2 x_3}$$

e

$$b_5 = \frac{x_3^2 + \alpha x_1^2 + \alpha^2 x_2^2}{x_3 + \alpha x_1 + \alpha^2 x_2} \qquad b_6 = \frac{x_3^2 + \alpha x_2^2 + \alpha^2 x_1^2}{x_3 + \alpha x_2 + \alpha^2 x_1}$$

ma ora, moltiplicando numeratore e denominatore di b_1 per α prima e per α^2 poi e servendosi ancora delle proprietà delle radici dell'unità si verifica che

$$b_1 = b_3 = b_5 \qquad \text{e} \qquad b_2 = b_4 = b_6$$

per cui l'equazione in b è ancora di sesto grado ma, precisamente, è il cubo di un'equazione di secondo grado: ancora una volta, l'analisi del comportamento di certe funzioni delle radici di (7.1) ha permesso di conoscere *a priori* cosa aspettarsi da un metodo di risoluzione.

Per concludere, ricordo che il risultato forse più importante ottenuto con il metodo di Tschirnhaus è la riduzione della più generale equazione di quinto grado alla forma

$$x^5 + ax + b = 0 \tag{7.17}$$

che sarà effettuata indipendentemente da Bring [8] e Jerrard [9][5]: più in generale, con lo stesso metodo si possono eliminare da un'equazione di grado m i coefficienti che moltiplicano x^{m-1}, x^{m-2}, x^{m-3}.

7.3 La risolvente di Lagrange

Lagrange, dopo aver trovato gli ingredienti comuni a tutti i metodi noti di soluzione delle equazioni algebriche fino al quarto grado, è in grado di proporre un approccio generale ed uniforme alla soluzione algebrica di tutte le equazioni che sarà destinato a funzionare per le equazioni fino al quarto grado e per le equazioni binomie. Per illustrare gli aspetti salienti del metodo di Lagrange mi servirò della Nota XIII, *Sur la résolution des équations algébriques* dell'edizione del 1808 del *Traité* [2] che appunto tratta dei principi generali del metodo. Il punto di partenza per la risoluzione algebrica di un'equazione generale del tipo

$$x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \cdots = 0 \tag{7.18}$$

le cui radici indicheremo con $\{x_1, x_2, \cdots x_{m-1}, x_m\}$ è l'osservazione che in tutti i metodi di soluzione noti si effettuava il ricorso ad un'equazione ausiliaria (ridotta o *risolvente*, nel *Traité*) le cui radici sono

$$t_0 = x_1 + \alpha x_2 + \cdots + \alpha^{m-2} x_{m-1} + \alpha^{m-1} x_m = \sum_{k=1}^{m} \alpha^{k-1} x_k \tag{7.19}$$

e tutte quelle che si ottengono da t_0 permutando in un modo arbitrario le radici di (7.18): dunque, a questo livello, la risolvente appare essere un'equazione di

[5] Erland Bring (1736-1798), matematico svedese e George Birch Jerrard (1804-1863), matematico britannico. È curioso osservare che Jerrard si occupò di questo problema perché nutriva dei dubbi sulla validità della dimostrazione di Abel circa l'impossibilità di risolvere equazioni algebriche di grado superiore al quarto.

grado $m! = m \cdot (m-1) \cdots 3 \cdot 2 \cdot 1$. In (7.19) α è una radice m-esima dell'unità, $\alpha \neq 1$. Vi è una differenza tecnica tra il caso in cui m è un numero primo oppure composto. Per brevità, ci soffermeremo nel seguito solo sul caso in cui m è *primo*. In questo caso, valgono una serie di proprietà di α che è bene rammentare visto il ruolo che giocheranno tra poco. Anzitutto, tutte le potenze α^k con k intero compreso tra 1 ed m sono diverse tra loro quando lo sono gli esponenti. Come conseguenza di deduce che tutte le potenze α^k, con $k = 1, \cdots m$ risolvono l'equazione binomia $y^m - 1 = 0$. Lagrange si serve di queste proprietà per ricavare un metodo potenzialmente in grado di risolvere equazioni di ogni grado. Infatti, tornando alla (7.19), Lagrange osserva che, se si effettua la permutazione ciclica $x_1 \mapsto x_2 \mapsto x_3 \cdots \mapsto x_{m-1} \mapsto x_m \mapsto x_1$, ecc.per la quale Lagrange *non* ha una specifica notazione, si ottiene

$$t_1 = x_m + \alpha x_1 + \cdots + \alpha^{m-3} x_{m-3} + \alpha^{m-2} x_{m-2} + \alpha^{m-1} x_{m-1}.$$

Allo stesso risultato tuttavia si perviene moltiplicando t_0 per α, grazie ad $\alpha^m = 1$. Similmente, la moltiplicazione di t_0 per $\alpha^k \quad (k = 1, \cdots m)$ non fa uscire dall'insieme ottenuto da t_0 permutando le radici della (7.18). Si deduce in questo modo che la risolvente, oltre ad avere il fattore $(t - t_0)$ dovrà avere anche i fattori $t - \alpha t_0$,...,$t - \alpha^k t_0$, $t - \alpha^{m-1} t_0$ e dunque, in definitiva, potrà contenere solo il fattore $t^m - t_0^m$. Un attimo di riflessione porta a concludere che le m permutazioni equivalenti alla moltiplicazione di t_0 per una potenza di α sono del tipo $x_h \mapsto x_{h+k} \bmod m$ e che tutte le permutazioni che lasciano invariato x_1 ma agiscono solo sulle rimanenti $m-1$ radici non possono essere tra loro equivalenti. Dunque, le $m!$ permutazioni tra le radici si fattorizzano in $(m-1)!$ gruppi di m permutazioni ciascuno, ed ogni gruppo porta in evidenza un termine t^m: la risolvente conterrà solo potenze di t^m per cui, posto $\theta := t^m$, l'equazione per θ sarà di grado $(m-1)!$ ed avrà come radici i diversi valori di θ che si ottengono permutando tra loro le radici $\{x_2, x_3, \cdots, x_m\}$. Siccome $\alpha^m = 1$, a conti fatti θ si esprimerà come

$$\theta = \xi_0 + \alpha \xi_1 + \alpha^2 \xi_2 + \cdots \alpha^{m-1} \xi_{m-1} \tag{7.20}$$

dove ora le ξ_k sono funzioni razionali delle $\{x_1, x_2, \cdots, x_{m-1}, x_m\}$ *invarianti* rispetto alle permutazioni del tipo $x_h \mapsto x_{h+k} \bmod m$. Lagrange compie l'osservazione cruciale che, note le ξ_k, le radici dell'equazione proposta (7.18) saranno note anch'esse. Infatti, considerando t_0 in (7.19) come funzione di α e delle $\{x_1, x_2, \cdots x_{m-1}, x_m\}$ ed indicando $t_0 = t(\alpha, \{x_k\}) =: \sqrt[m]{\theta_1}$, si potrà scrivere

$$\left\{ \begin{array}{lcccccccccc} t(1, \{x_k\}) = & x_1 & + & x_2 & + & \cdots & + & x_m & = & \sqrt[m]{\theta_0} \\ t(\alpha, \{x_k\}) = & x_1 & + & \alpha x_2 & + & \cdots & + & \alpha^{m-1} x_m & = & \sqrt[m]{\theta_1} \\ t(\beta, \{x_k\}) = & x_1 & + & \beta x_2 & + & \cdots & + & \beta^{m-1} x_m & = & \sqrt[m]{\theta_2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ t(\lambda, \{x_k\}) = & x_1 & + & \lambda x_2 & + & \cdots & + & \lambda^{m-1} x_m & = & \sqrt[m]{\theta_{m-1}} \end{array} \right. \tag{7.21}$$

dove $1, \alpha, \beta, \cdots \lambda$ sono tutte le m radici m-esime dell'unità e dunque sono soluzioni dell'equazione $x^m - 1 = 0$ che avendo tutti i termini intermedi nulli gode,

grazie ai teoremi newtoniani, delle seguenti proprietà:

$$1 + \alpha + \beta + \cdots + \lambda = 0,$$

$$1 + \alpha^2 + \beta^2 + \cdots + \lambda^2 = 0$$

e così via fino a

$$1 + \alpha^{m-1} + \beta^{m-1} + \cdots + \lambda^{m-1} = 0.$$

Se allora sommiamo tra loro le (7.21) ed utilizziamo queste proprietà otteniamo

$$x_1 = \frac{\sqrt[m]{\theta_0} + \sqrt[m]{\theta_1} + \sqrt[m]{\theta_2} + \cdots + \sqrt[m]{\theta_{m-1}}}{m}.$$

Similmente, se si moltiplica la seconda delle (7.21) per α^{m-1}, la terza per β^{m-1} e così via fino all'ultima che viene moltiplicata per λ^{m-1} e poi si sommano le equazioni così ottenute si ha

$$x_2 = \frac{\sqrt[m]{\theta_0} + \alpha^{m-1}\sqrt[m]{\theta_1} + \beta^{m-1}\sqrt[m]{\theta_2} + \cdots + \lambda^{m-1}\sqrt[m]{\theta_{m-1}}}{m} :$$

in generale,

$$x_k = \frac{\sqrt[m]{\theta_0} + \alpha^{m-k+1}\sqrt[m]{\theta_1} + \beta^{m-k+1}\sqrt[m]{\theta_2} + \cdots + \lambda^{m-k+1}\sqrt[m]{\theta_{m-1}}}{m}.$$

Il problema è ora ricondotto alla determinazione delle ξ_k, precisamente a stabilire il grado dell'equazione soddisfatta da queste quantità ed alla determinazione dei coefficienti di queste equazioni. Per questo Lagrange osserva che, sostituire α ad un'altra radice m-esima dell'unità distinta da 1 in $t(\alpha, \{x_k\})$ equivale a rimpiazzare x_2 con una delle altre $m-2$ radici x_3, x_4, ..., x_m. Dunque le $(m-1)!$ permutazioni che danno luogo a fattori distinti nella ridotta si possono raggruppare ad $(m-1)$ ad $(m-1)$ ottenendo così un numero di $(m-2)!$ permutazioni non equivalenti tra le radici di (7.18). Si può allora concludere che i coefficienti ξ_k sono radici di equazioni di grado $m-1$ i cui coefficienti però dipendono da equazioni di grado $(m-2)!$. Purtroppo, non appena $m = 5$, $(m-2)! = 3! = 6 > 5$ e dunque non si può sperare in una risolvente che sia più facile da risolvere rispetto alla (7.18). Lagrange in effetti, trova direttamente i coefficienti dell'equazione in θ che ha come radici le θ_1, ...,θ_{m-1} ([2], pp. 305-307) ed uno di questi dipende da un'equazione di grado $(m-2)!$ mentre tutti gli altri sono determinabili grazie ai teoremi newtoniani. Il metodo permette però di ottenere l'espressione in radicali delle equazioni ciclotomiche $x^m - 1 = 0$ in modo diretto, indipendente dalla tecnica proposta da Gauss nelle *Disquisitiones Arithmeticae* del 1801. Lagrange illustra l'applicazione del metodo alle equazioni ciclotomiche di grado m primo nella Nota XIV del *Traité* [2].

Questo è, in estrema sintesi, il cuore del lavoro di Lagrange sulla risoluzione algebrica delle equazioni, un lavoro che influenzerà molti studiosi come Paolo Ruffini [10] che mutuerà le tecniche di Lagrange per dimostrare, pur con qualche mancanza, l'impossibilità di risolvere algebricamente in generale un'equazione

di grado superiore al quarto o come Louis-Augustin Cauchy che svilupperà a più riprese nella sua carriera i risultati di Lagrange e Ruffini sul gruppo delle permutazioni o, ancora, come Évariste Galois che dalla lettura di Lagrange trarrà spunto per gettare le basi della teoria che oggi porta il suo nome.

7.4 Vandermonde e le equazioni ciclotomiche

Il francese Alexandre-Théophile Vandermonde (1735-1796) fu un personaggio eclettico: matematico, musicista, studioso di economia politica [11]. Nella storia delle equazioni algebriche egli entra a pieno titolo per una importante memoria, *Mémoire sur la résolution des équations* [12], coeva alle *Réflexions* di Lagrange ma apparsa qualche tempo dopo queste a causa di un notevole ritardo nella pubblicazione tra le *Memorie* dell'Accademia delle Scienze di Parigi. La memoria di Vandermonde si può in effetti suddividere in due parti e contiene molte idee vicine a quelle contenute nelle *Réflexions*, come Lagrange stesso riconobbe nella Nota XIII del *Traité* [2] appena esaminata. Nella prima parte di [12], molto estesa, Vandermonde mira ad ottenere un'espressione di ciascuna radice di un'equazione assegnata in funzione di tutte le radici dell'equazione stessa. Nella seconda parte, su cui concentriamo l'attenzione in questa sezione seguendo l'esposizione di Tignol [13], egli trova l'espressione in *radicali* delle soluzioni dell'equazione ciclotomica $x^{11} - 1 = 0$ servendosi di un metodo che contiene in forma embrionale alcune delle idee che saranno sviluppate cinquant'anni più tardi ed in modo del tutto indipendente da Galois.

Vandermonde osserva come sia inevitabile la presenza di una certa ambiguità in ogni formula risolutiva che si voglia considerare in quanto, attraverso un'unica formula, si vogliono ottenere tutte le radici di un'equazione assegnata. La via battuta da Vandermonde per ottenere una formula risolutiva si snoda in tre parti:

1) Trovare una funzione $F_n(x_1, x_2, \cdots, x_n)$ delle radici $\{x_i\} \equiv \{x_1, x_2, \cdots x_{n-1}, x_n\}$ di un'equazione di grado n che permetta di esprimere *tutte le radici*.

2) Porre la funzione appena determinata in una forma invariante rispetto allo scambio delle radici.

3) Servirsi delle formule di Viète-Girard per esprimere la funzione trovata ai passi precedenti in termini dei coefficienti dell'equazione proposta. A questo proposito, ricordiamo che Vandermonde dimostrò in generale che ogni funzione simmetrica di $\{x_1, x_2, \cdots x_{n-1}, x_n\}$ si può esprimere in funzione dei coefficienti dell'equazione proposta.

Vandermonde propose di considerare la funzione

$$V_i(x_1, x_2, \cdots, x_n) = \varrho_1^i x_1 + \varrho_2^i x_2 + \cdots + \varrho_{n-1}^i x_{n-1} + \varrho_n^i x_n \tag{7.22}$$

che gioca un ruolo del tutto analogo rispetto alla risolvente di Lagrange. In (7.22) $i = 1, 2, \cdots, n-1$, le ϱ_k sono le radici n-esime dell'unità e la formula

risolutiva proposta da Vandermonde è

$$F_n(x_1, x_2, \cdots x_n) = \frac{1}{n}\left[\sum_{i=1}^{n} x_i + \sum_{i=1}^{n-1} \sqrt[n]{V_i^n(x_1, x_2, \cdots, x_n)}\right] \tag{7.23}$$

dove tutte le singole radici vengono ottenute a patto di scegliere un'opportuna determinazione delle radici n-esime delle funzioni V_i^n. Ad esempio, se si vuole ottenere x_k si sceglie $\sqrt[n]{V_i^n(x_1, x_2, \cdots, x_n)} = \varrho_k^{-i} V_i(x_1, x_2, \cdots, x_n)$ in quanto da (7.22) si ricava

$$\sqrt[n]{V_i^n(x_1, x_2, \cdots, x_n)} = x_k + \sum_{j \neq k} \left(\varrho_j \varrho_k^{-1}\right)^i x_j$$

e dunque da (7.23) si ha

$$F_n(x_1, x_2, \cdots x_n) = x_k + \sum_{j \neq k}\left[\sum_{i=0}^{n-1}\left[\left(\varrho_j \varrho_k^{-1}\right)^i\right] x_j\right] \tag{7.24}$$

dove l'indice nella sommatoria su i parte da 0 dal momento che si è riscritto

$$\sum_{j \neq k} x_j = \sum_{j \neq k} \left(\varrho_j \varrho_k^{-1}\right)^0 x_j.$$

Si osserva ora che, quando $j \neq k$, $\varrho_j \varrho_k^{-1}$ è anch'essa una radice n-esima dell'unità distinta da 1 e dunque risolve l'equazione

$$x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x^2 + x + 1 = \sum_{i=0}^{n-1} x^i = 0$$

che dimostra come la somma doppia in (7.24) sia nulla per cui, con *questa* determinazione di $\sqrt[n]{V_i^n(x_1, x_2, \cdots, x_n)}$ si ha $F(x_1, x_2, \cdots x_n) = x_k$. Osserviamo che, nonostante l'apparente diversità, la risolvente impiegata da Vandermonde coincide con quella introdotta da Lagrange.

Veniamo ora allo studio dell'equazione ciclotomica

$$x^{11} - 1 = 0 \tag{7.25}$$

di cui Vandermonde mostra la risolubilità in termini di radicali algebrici. Quest'ultima specificazione è essenziale dal momento che era noto da tempo come ottenere la rappresentazione *trigonometrica* complessa per le radici di equazioni del tipo $x^n - 1 = 0$. Al contrario, la risolubilità in termini di radicali era dimostrata solo fino ad $n = 10$ ed il grande merito di Vandermonde fu quello di risolvere il caso $n = 11$ che, come vedremo tra poco, conduce ad un'equazione di *quinto* grado per la quale non esiste in generale una formula risolutiva. Anzitutto ricordiamo che, liberata la (7.25) dalla radice evidente $x = 1$, l'equazione da risolvere è

$$x^{10} + x^9 + \cdots + x^2 + x + 1 = 0. \tag{7.26}$$

Ora, quando n è un numero primo maggiore di 2, de Moivre aveva escogitato un artificio che consentiva di ridurre il grado dell'equazione $x^n - 1 = 0$ che, eliminata la radice $x = 1$ e posto $n = 2p + 1$, diviene

$$x^{2p} + x^{2p-1} + \cdots + x + 1 = 0. \tag{7.27}$$

Dividendo tutti i termini per x^p e raggruppando i termini a due a due procedendo simetricamente a partire dagli estremi, (7.27) si riscrive come

$$\left(x^p + \frac{1}{x^p}\right) + \left(x^{p-1} + \frac{1}{x^{p-1}}\right) + \cdots + \left(x^2 + \frac{1}{x^2}\right) + \left(x + \frac{1}{x}\right) + 1 = 0. \tag{7.28}$$

Posto

$$y := x + \frac{1}{x} \tag{7.29}$$

non è difficile verificare che, definito

$$s_p := x^p + \frac{1}{x^p},$$

vale la relazione ricorsiva

$$s_{p+1} = ys_p - s_{p-1}. \tag{7.30}$$

avendo cura di porre $s_0 = 2$ ed $s_1 = y$. Nel caso che ci interessa si ha $p = 5$ ed uso ripetuto di (7.30) consente di ricavare

$$x^2+\frac{1}{x^2} = y^2-2 \quad x^3+\frac{1}{x^3} = y^3-3y \quad x^4+\frac{1}{x^4} = y^4-4y^2+2 \quad x^5+\frac{1}{x^5} = y^5-5y^3+5y$$

che permette di trasformare (7.26) in

$$y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1 = 0.$$

Vandermonde, nell'applicare il metodo di de Moivre esprime (7.26) in termini di $X = -y$ per cui l'equazione ciclotomica da risolvere è

$$X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1 = 0. \tag{7.31}$$

Ora, è noto che le radici $x_k \neq 1$ 11-esime dell'unità, soluzioni di (7.26), si esprimono come $x_k = \mathrm{e}^{\frac{2k\pi i}{11}}$, con $k = 1, \cdots, 10$ e dunque le soluzioni di (7.31) si possono scrivere come

$$X_1 = -2\cos\frac{2\pi}{11} \quad X_2 = -2\cos\frac{4\pi}{11} \quad X_3 = -2\cos\frac{6\pi}{11} \quad X_4 = -2\cos\frac{8\pi}{11} \quad X_5 = -2\cos\frac{10\pi}{11},$$

come è facile verificare in quanto

$$x_k + \frac{1}{x_k} = y_k = -X_k = \mathrm{e}^{\frac{2k\pi i}{11}} + \mathrm{e}^{-\frac{2k\pi i}{11}} = 2\cos\frac{2k\pi}{11}.$$

Vandermonde, applicando la formula di prostaferesi

$$2\cos\alpha\cos\beta = \cos(\alpha+\beta) + \cos(\alpha-\beta) \tag{7.32}$$

al caso $\alpha = \beta = \frac{2\pi}{11}$ ottiene

$$2\cos^2\left(\frac{2\pi}{11}\right) = \cos\left(\frac{4\pi}{11}\right) + 1$$

che si può esprimere in termini delle radici di (7.31)

$$X_1^2 = 2 - X_2 : \tag{7.33}$$

similmente, se si riapplica (7.32) prendendo $\alpha = \beta$ coincidente con uno degli argomenti dei coseni che figurano nelle X_k si possono ottenere le relazioni

$$X_2^2 = 2 - X_4 \quad X_3^2 = 2 - X_5 \quad X_4^2 = 2 - X_3 \quad X_5^2 = 2 - X_1. \tag{7.34}$$

Quando invece si applica (7.32) prendendo valori distinti di α e β, entrambi argomenti di coseni che compaiono nelle X_k, si ottengono altre relazioni tra le radici

$$X_1X_2 = -(X_1+X_3) \quad X_2X_3 = -(X_1+X_5) \quad X_3X_4 = -(X_1+X_4) \quad X_4X_5 = -(X_1+X_2). \tag{7.35}$$

Vandermonde osserva ora che, se su queste relazioni si opera la permutazione

$$\sigma := \begin{pmatrix} X_1 & X_2 & X_3 & X_4 & X_5 \\ X_2 & X_4 & X_5 & X_3 & X_1 \end{pmatrix},$$

le relazioni (7.34) vengono scambiate tra di loro mentre le (7.35) vengono mutate in altre ancora valide. È importante osservare che, a differenza delle formule di Viète-Girard che sono invarianti sotto l'azione di *qualsiasi* permutazione, le relazioni appena trovate lo sono solo per un *sottogruppo* del gruppo di permutazioni di n elementi. La differenza è cruciale perché, come farà vedere più tardi Galois, la riduzione del gruppo che lascia invariate certe relazioni tra le radici è la chiave per decidere se un'equazione algebrica sia o meno risolubile in termini di radicali. In altri termini, mentre la simmetria insita nelle formule di Viète-Girard impedisce di discriminare tra loro le radici, la presenza di relazioni tra le radici di un'equazione che siano invarianti sotto l'azione di sottogruppi sempre più piccoli del gruppo delle permutazioni, permette di distinguere tra loro le radici e dunque di condurre alla risolubilità per radicali di quest'ultima.

Per vedere come Vandermonde proceda nella risoluzione per radicali di (7.26) notiamo come relazioni del tipo (7.34) ed (7.35) permettono di abbassare il grado di un polinomio nelle X_k. Supponiamo infatti che in un polinomio figuri il termine X_1^5. Applicando (7.33), (7.34) ed (7.35) si può scrivere

$$\begin{aligned} &X_1^5 = X_1^2 \cdot X_1^2 \cdot X_1 = (2 - X_2)^2 X_1 = (4 - 4X_2 + X_2^2)X_1 = \\ &4X_1 + 4(X_1 + X_3) - X_2(X_1 + X_3) = 10X_1 + 5X_3 + X_5 : \end{aligned}$$

seguendo un procedimento analogo è possibile sempre ridurre un polinomio nelle X_k ad un altro polinomio di *primo* grado. Grazie a questa osservazione, Vandermonde riesce a semplificare notevolmente l'espressione delle funzioni V_i^5 che

compaiono in (7.23). Infatti, per quanto appena esemplificato

$$\begin{aligned}&V_i(X_1,X_2,X_3,X_4,X_5)^5=(\varrho_1^iX_1+\varrho_2^iX_2+\varrho_3^iX_3+\varrho_4^iX_4+\varrho_5^iX_5)^5\\&=A_1(\{\varrho_k\})X_1+A_2(\{\varrho_k\})X_2+A_3(\{\varrho_k\})X_3+A_4(\{\varrho_k\})X_4+A_5(\{\varrho_k\})X_5+A_6(\{\varrho_k\})\end{aligned}\tag{7.36}$$

dove i coefficienti A_i dipendono dalle radici quinte dell'unità $\{\varrho_k\}\equiv\{\varrho_1,\varrho_2,\varrho_3,\varrho_4,\varrho_5\}$. Se ora eseguiamo ripetutamente su V_i^5 la permutazione σ otterremo

$$\begin{aligned}V_i(X_2,X_4,X_5,X_3,X_1)^5=\;&A_1(\{\varrho_k\})X_2+A_2(\{\varrho_k\})X_4+A_3(\{\varrho_k\})X_5\\&+A_4(\{\varrho_k\})X_3+A_5(\{\varrho_k\})X_1+A_6(\{\varrho_k\})\end{aligned}\tag{7.37}$$

$$\begin{aligned}V_i(X_4,X_3,X_1,X_5,X_2)^5=\;&A_1(\{\varrho_k\})X_4+A_2(\{\varrho_k\})X_3+A_3(\{\varrho_k\})X_1\\&+A_4(\{\varrho_k\})X_5+A_5(\{\varrho_k\})X_2+A_6(\{\varrho_k\})\end{aligned}\tag{7.38}$$

$$\begin{aligned}V_i(X_3,X_5,X_2,X_1,X_4)^5=\;&A_1(\{\varrho_k\})X_3+A_2(\{\varrho_k\})X_5+A_3(\{\varrho_k\})X_2\\&+A_4(\{\varrho_k\})X_1+A_5(\{\varrho_k\})X_4+A_6(\{\varrho_k\})\end{aligned}\tag{7.39}$$

e

$$\begin{aligned}V_i(X_5,X_1,X_4,X_2,X_3)^5=\;&A_1(\{\varrho_k\})X_5+A_2(\{\varrho_k\})X_1+A_3(\{\varrho_k\})X_4\\&+A_4(\{\varrho_k\})X_2+A_5(\{\varrho_k\})X_3+A_6(\{\varrho_k\}).\end{aligned}\tag{7.40}$$

Ora, le proprietà generali delle radici n-esime dell'unità con n numero primo implicano che sia sempre possibile esprimere tutte le ϱ_k come potenze di un'*unica* radice n-esima $\omega\neq 1$. Nulla impedisce di numerare le radici in modo che sia

$$\varrho_1=1\quad\varrho_2=\omega\quad\varrho_4=\omega^2\quad\varrho_3=\omega^3\quad\varrho_5=\omega^4$$

e dunque

$$V_i(X_1,X_2,X_3,X_4,X_5)=X_1+\omega^iX_2+\omega^{2i}X_4+\omega^{3i}X_3+\omega^{4i}X_5.$$

Se ora applichiamo la permutazione σ otteniamo

$$\begin{aligned}&V_i(X_2,X_4,X_5,X_3,X_1)=X_2+\omega^iX_4+\omega^{2i}X_3+\omega^{3i}X_5+\omega^{4i}X_1=\\&\omega^{-i}[X_1+\omega^iX_2+\omega^{2i}X_4+\omega^{3i}X_3+\omega^{4i}X_5]=\omega^{-i}V_i(X_1,X_2,X_3,X_4,X_5)\end{aligned}$$

e quindi, siccome $\omega^{5i}=\omega^{-5i}=1$ si ottiene, iterando la permutazione σ

$$\begin{aligned}&V_i(X_1,X_2,X_3,X_4,X_5)^5=V_i(X_2,X_4,X_5,X_3,X_1)^5=V_i(X_4,X_3,X_1,X_5,X_2)^5=\\&=V_i(X_3,X_5,X_2,X_1,X_4)^5=V_i(X_5,X_1,X_4,X_2,X_3)^5\end{aligned}$$

per cui, sommando tra loro (7.36)-(7.40), si ottiene

$$V_i(X_1,X_2,X_3,X_4,X_5)^5=\frac{1}{5}(A_1+A_2+A_3+A_4+A_5)(X_1+X_2+X_3+X_4+X_5)+A_6$$

ovvero, ricordando che per (7.31) $X_1+X_2+X_3+X_4+X_5=1$

$$V_i(X_1,X_2,X_3,X_4,X_5)^5=\frac{1}{5}(A_1+A_2+A_3+A_4+A_5)+A_6$$

che risolve il problema della soluzione per radicali dell'equazione (7.25) visto che le quantità $A_1 \cdots, A_6$ sono funzioni note delle radici quinte dell'unità ϱ_k che sono esprimibili per radicali (cfr. *e.g.* [1], p. 253):

$$\begin{aligned}
\varrho_1 &= 1 \\
\varrho_2 &= \tfrac{\sqrt{5}-1}{4} + \tfrac{\sqrt{10+2\sqrt{5}}}{4} i \\
\varrho_3 &= \tfrac{\sqrt{5}-1}{4} - \tfrac{\sqrt{10+2\sqrt{5}}}{4} i \\
\varrho_4 &= -\tfrac{\sqrt{5}+1}{4} + \tfrac{\sqrt{10-2\sqrt{5}}}{4} i \\
\varrho_5 &= -\tfrac{\sqrt{5}+1}{4} - \tfrac{\sqrt{10-2\sqrt{5}}}{4} i
\end{aligned}$$

Vandermonde, senza dare alcuna idea della dimostrazione, asserisce che quant mostrato in dettaglio per $n = 11$ vale anche per tutti i numeri primi maggiori di 11. Questo risultato sarà ritrovato da Gauss, trent'anni più tardi, nelle *Disquisitiones Arithmeticae* con tecniche di teoria dei numeri. Vandermonde non sembra essersi occupato più dell'argomento ed il suo lavoro non sembra avere influito su Gauss, che pure ne era a conoscenza [11]. Quanto a Lagrange, nella Nota XIII del *Traité* [2] egli attribuisce a Vandermonde la giusta lode. L'aspetto più significativo che si può cogliere dal lavoro di Vandermonde è l'osservazione che, grazie all'esistenza di certe relazioni tra le radici invarianti rispetto ad un sottogruppo (terminologia sconosciuta a Vandermonde) del gruppo delle permutazioni, e non già rispetto all'intero gruppo delle permutazioni, è possibile risolvere per radicali l'equazione ciclotomica (7.25). Questa idea verrà sviluppata in modo organico da Galois, anche se questi non citerà mai Vandermonde ed appare dunque possibile che non conoscesse il suo lavoro se non forse per l'accenno che ne fa Lagrange nel *Traité*.

7.5 Appendice I

In questa sezione di complemento, dimostriamo i teoremi o formule newtoniane che consentono di trovare la somma delle potenze k-esime delle radici di un'equazione algebrica. La dimostrazione è condotta sulla falsariga di [14], Cap. VII. Consideriamo l'equazione a coefficienti reali

$$p(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots a_{n-1} x + a_n = 0 \tag{7.41}$$

e siano x_1, x_2,...,x_n le sue radici, eventualmente complesse. Introduciamo le somme delle potenze k-esime delle radici di $p(x) = 0$

$$s_k = \sum_{i=1}^{n} x_i^k. \tag{7.42}$$

Per definizione di radice di un'equazione algebrica possiamo scrivere

$$p(x) = (x - x_1)(x - x_2) \cdots (x - x_{n-1})(x - x_n)$$

ed osservare che

$$p'(x) = \frac{p(x)}{x - x_1} + \frac{p(x)}{x - x_2} + \cdots + \frac{p(x)}{x - x_n}.$$

Ora i quozienti che compaiono a destra di questa equazione possono essere determinati esattamente grazie al principio di identità dei polinomi per cui, ad esempio,

$$\frac{p(x)}{x - x_1} = x^{n-1} + (x_1 + a_1)x^{n-2} + (x_1^2 + x_1 a_1 + a_2)x^{n-3} + \cdots + (x_1^k + a_1 x_1^{k-1} + a_2 x_1^{k-2} + \cdots + a_k)x^{n-k-1} + \cdots .$$

Trovati similmente tutti gli altri quozienti e dopo aver sommato i risultati si ottiene, grazie anche a (7.42),

$$p'(x) = nx^{n-1} + (s_1 + na_1)x^{n-2} + (s_2 + s_1 a_1 + na_2)x^{n-3} + \cdots + (s_k + a_1 s_{k-1} + a_2 s_{k-2} + \cdots + na_k)x^{n-k-1} + \cdots .$$

D'altra parte, se deriviamo partendo da (7.41), otteniamo

$$p'(x) = nx^{n-1} + (n-1)a_1 x^{n-2} + (n-2)a_2 x^{n-3} + \cdots + a_{n-1}$$

ed ugualiando le potenze ad ugual esponente di x nelle due espressioni di $p'(x)$ otteniamo

$$s_1 = -a_1, \qquad s_2 = -a_1 s_1 - 2a_2 = a_1^2 - 2a_2$$

e, per $k < n$

$$s_k + a_1 s_{k-1} + a_2 s_{k-2} + \cdots + a_n s_{n-k} + \cdots + ka_k = 0$$

che, ricorsivamente, si può risolvere esprimendo s_k in funzione dei coefficienti di (7.41). I casi $k \geq n$ o $k < 0$ possono essere trattati con opportuni artifici per i quali rimando a [14], pp. 85–86. È importante osservare che le s_k sono funzioni razionali dei coefficienti di (7.41).

7.6 Appendice II

Mostriamo, ancora seguendo [14], §70, il teorema fondamentale sulle funzioni simmetriche delle radici di un'equazione algebrica come (7.41)

Teorema *Ogni funzione razionale simmetrica delle radici di un'equazione algebrica è in realtà esprimibile in funzione dei coefficienti dell'equazione stessa.*

Dim. Consideriamo il prodotto $s_m s_p$ nel caso $m \neq p$: da (7.42) abbiamo

$$s_m s_p = x_1^{m+p} + x_2^{m+p} + \cdots + x_n^{m+p} + x_1^m x_2^p + x_1^m x_3^p + \cdots + x_2^m x_3^p + \cdots$$

e dunque

$$s_m s_p - s_{m+p} = \sum x_j^m x_k^p$$

dove la somma è intesa su tutti i valori di j e k, con $j \neq k$ ed è dunque una funzione simmetrica delle radici di (7.41). Dunque, nel caso $m \neq p$, somme del

tipo $\sum x_j^m x_k^p$ sono esprimibili solo in termini di s_k che sappiamo essere funzioni solo dei coefficienti di (7.41). Se $m = p$ allora è facile verificare che

$$\sum x_j^m x_k^p = 2\sum (x_j x_k)^m = s_m^2 - s_{2m}$$

ed il teorema è ancora valido. Consideriamo ora somme del tipo

$$\sum x_j^m x_k^p x_\ell^q$$

dove la somma è intesa su tutte le terne $j \neq k \neq \ell$. Ora, ricordando (7.42), abbiamo

$$\begin{array}{l} s_q \sum x_j^m x_k^p = x_1^{m+q} x_2^p + x_2^{m+q} x_3^p + \cdots + x_3^{m+q} x_1^p + \cdots \\ + x_1^m x_2^{p+q} + + x_2^m x_3^{p+q} + + x_3^m x_1^{p+q} + \cdots \\ + + x_1^m x_2^p x_3^q + \cdots \end{array}$$

ed i termini su ogni riga a destra del segno di uguaglianza corrispondono, rispettivamente a $\sum x_j^{m+q} x_k^p$, $\sum x_j^m x_k^{p+q}$ e $\sum x_j^m x_k^p x_\ell^q$. Usando i risultati ottenuti al passo precedente possiamo concludere

$$\sum x_j^m x_k^p x_\ell^q = s_m s_p s_q - s_{m+p} s_q - s_{m+q} s_p - s_m s_{p+q} + 2 s_{m+p+q}$$

che ancora mostra il teorema, almeno nel caso $j \neq k \neq \ell$. Se almeno due di questi indici coincidono, il risultato permane. Dovrebbe essere chiaro che, iterando il processo e considerando funzioni simmetriche che coinvolgono ad ogni passo una radice in più di quelle del passo precedente, il teorema è dimostrabile per tutte le funzioni simmetriche delle radici di (7.41) *omogenee*. Se la funzione non è omogenea, basta applicare il teorema ad ogni termine omogeneo presente in essa. Infine, se si ha un quoziente tra funzioni simmetriche, sia il numeratore che il denominatore debbono separatamente essere funzioni simmetriche e dunque il teorema è dimostrato per tutte le funzioni razionali simmetriche delle radici di (7.41).

Bibliografia

[1] J.L. Lagrange: Réflexions sur la résolution algébrique des équations, *Nouveaux Mém. de l'Acad. des Sciences et Belles-Lettres de Berlin*, **1**, 134–215, (1770); **2**, 138-253, (1771). In *Œuvers Complètes*, vol. 3, J.A. Serret, Ed., Gauthier-Villars, Paris, (1869), 205-421.

[2] J.L. Lagrange: Traité de la résolution des équations numériques de tous les degrés, avec des notes sur pluiseurs points de la Théorie des équations algébriques, Courcier, Paris, (1808). In *Œuvers Complètes*, vol. 8, J.A. Serret, Ed., Gauthier-Villars, Paris, (1879), 11-370.

[3] R.R. Hamburg: The theory of equations in the 18th century: the work of Joseph Lagrange. *Archive for History of Exact Sciences*, **13**, (1976), 17–36.

[4] B.M. Kiernan: The development of Galois theory from Lagrange to Artin. *Archive for History of Exact Sciences*, **13**, (1971), 40–154.

[5] J. Pierpont: Lagrange's place in the theory of substitutions. *Bull. Amer. Math. Soc.*, **1**, 196–204, (1894).

[6] L. Euler: De fractionibus continuis dissertatio. *Commentarii Academiae Scientiarum Petropolitanae* **9** (1744), 98-137.

[7] E.W. Graf von Tschirnhaus: Methodus auferendi omnes terminos intermedios ex data aequatione. *Acta Eruditorum*, **2**, 204–207, (1683).

[8] E. Bring: *Melemata quaedam mathematica circa transformationem aequationum algebraicarum*, Lund, (1786).

[9] G.B. Jerrard: *An Essay on the Resolution of Equations*, Taylor & Francis, London, (1858).

[10] P. Ruffini, *Teoria generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto.* Bologna, Stamperia di S. Tommaso d'Aquino, (1799). In *Opere Matematiche di Paolo Ruffini* a cura di E. Bortolotti, vol. 1, Cremonese, Roma, (1953).

[11] H. Lebesgue: L'œuvre mathématique de Vandermonde. *L'Einsegnement Mathématique*, **1** (S. 2), 201–223, (1955)

[12] A.T. Vandermonde: Mémoire sur la résolution des équations. *Histoire de l'Acad. des Sciences*, 365–416, (1771)

[13] J.-P. Tignol: *Galois' Theory of Algebraic Equations.* World Scientific, Singapore, (2001).

[14] F. Cajori: *An Introduction to the Modern Theory of Equations.* MacMillan, London, (1919).